Quantum Computers: The Need for a New Cryptographic Strategy

Chapter · July 2023

DOI: 10.1007/978-3-031-39542-0_7

3 authors, including:

Britta Hale
Naval Postgraduate School
21 PUBLICATIONS **167** CITATIONS
SEE PROFILE

Douglas Lee Van Bossuyt
Naval Postgraduate School
135 PUBLICATIONS **936** CITATIONS
SEE PROFILE

Quantum Computers: The Need for a New Cryptographic Strategy

Britta Hale, Nina Bindel, and Douglas L. Van Bossuyt

1 Introduction

"Quantum computing" is a term filled with both enigma and possibility—but one with very concrete potential effects on the security and stability of daily life. The word "quantum" refers to the smallest possible unit of quantity, and finessing our current computation approaches to achieve even finer-grained control is certainly an intriguing possibility. Thus, it is no surprise that quantum computing is an area of research and development attracting both investors and startups [36, 58, 90, 98]. For all systems, including industrial control systems (ICS), government systems, and defense systems, quantum computing offers not only opportunity but also risk. One of the capabilities that a quantum computer presents includes breaking of certain cryptographic primitives in their current form [61]. Cryptography—the backbone of security infrastructures around the world—propels even the slightest risk into magnified focus [92, 101]. In this chapter, we provide an overview of the risk of quantum computing to security and considerations to weigh in system hardening for quantum resistance, with tailoring to a strategic management and governance audience. Specifically, we provide context that decision-makers and engineers can use in preparing for the coming quantum threat with consideration to the amount of time needed to update existing fielded systems to meet the threat, as well as systems still to be developed.

B. Hale (✉) · D. L. Van Bossuyt
Naval Postgraduate School, Monterey, CA, USA
e-mail: britta.hale@nps.edu; douglas.vanbossuyt@nps.edu

N. Bindel
SandboxAQ, Palo Alto, CA, USA
e-mail: nina.bindel@sandboxaq.com

K. P. Balomenos et al. (eds.), *Handbook for Management of Threats*, Springer Optimization and Its Applications 205,
https://doi.org/10.1007/978-3-031-39542-0_7

In the remainder of this section, we provide high-level background information on cryptography and quantum computing to set the stage for the remainder of the chapter. We further outline the rest of the chapter at the end of this section.

1.1 Cryptography

Cryptography is a science and art based on extrapolating a little secret information to build larger architectures of security. For example, encryption offers the property of confidentiality, under which an attacker is unable to read data; it provides confidentiality through use of a small amount of secret information, that is, an encryption key. Only parties privy to the decryption key can access the data. Confidentiality is an important security goal when, for example, data is stored or communicated across networks [106]. Other important security properties offered by cryptography include authenticity and integrity. Algorithms providing authenticity and integrity, for example, *message authentication codes* and *digital signatures*, ensure that only parties with access to a secret key (authenticity) can modify the data (integrity), thus preventing forgeries and data manipulation [57].

Cryptography can be further divided into symmetric techniques (where a sender and receiver both have a copy of the same secret key) and asymmetric techniques (where only one party has the secret decryption key and all other parties have access to a *public* encryption key). Asymmetric encryption, also called public key encryption, allows anyone to send an encrypted message while only the holder of the secret key can decrypt, much like a drop-box. In contrast, for symmetric encryption, both parties use the same secret key for encryption and decryption. Usually symmetric encryption is used to store data, while for data in transit a mix of both—symmetric and asymmetric techniques—is used. More specifically, asymmetric techniques are used to exchange/agree on the secret key, which is then used to encrypt the data using symmetric techniques.

Asymmetric authentication can be achieved through digital signatures, with which one party signs data using a secret signing key (known only to the signer) while anyone (using a public verification key) can verify the signature. Likewise, there are corresponding symmetric techniques for when both parties possess a secret authentication key [97]. There is any entire field of research on cryptographic techniques and properties [62]; the above context suffices as a high-level introduction for the reader to this chapter.

1.2 Quantum Computers

Compared to our current transistor-based computers that compute over bits with state 0 or 1, quantum computers use the principles of quantum physics for computations. More concretely, this new generation of computers saves, processes,

and communicates data in the form of quantum states, also called qubits. While small quantum computers can already be built, such as Google's 72-qubit quantum computer [54], this technology is still in its infancy. To be of serious risk, for example, to break certain instances of deployed cryptographic algorithms, several million qubits are necessary [37]. While the difference between 72 and several million qubits seems huge, quantum computing experts estimate that quantum computers large enough to break certain currently used cryptographic algorithms will be built within the next 14 to 30 years [65]. However, as stated by the National Institute for Standard and Technology (NIST) [19], "Historically, it has taken almost two decades to deploy our modern public key cryptography infrastructure. Therefore, regardless of whether we can estimate the exact time of the arrival of the quantum computing era, we must begin now to prepare our information security systems to be able to resist quantum computing." Consequently, we take a closer look at system security implications of a quantum computer, the urgency of system transition, and key considerations for preparing for the transition to quantum resistance in complex systems.

1.3 When Systems Rely on Broken Cryptography

The importance of ensuring systems are operating with modern cryptography can be illustrated by issues with video feed hacks of uncrewed aerial systems (UASs). At least one incident of a UAS video feed being hacked is recorded in the open literature where an adversary was able to use the hacked video feed to injure or kill defense forces [56]. In such situations even if a UAS is only providing intelligence, surveillance, and reconnaissance (ISR), and has no weapons aboard, the ISR information can be damaging to national security and with potentially deadly outcomes. Thus, while it may be tempting to use old UAS systems especially in times of crisis, it is important to ensure cryptography is current so that unintended consequences do not occur. Further, any system that contains digital information should be protected to ensure the data is safe today and in the future. The following sections will investigate what this means for systems in the context of a quantum attack, extending the illustrated context of a classic attack on cryptography.

1.4 Outline

This chapter discusses how the threat of quantum computing impacts security for current systems and what considerations should be taken into account when preparing for it. As such, we start with explaining what the quantum threat is in Sect. 2. More concretely, we explain the implications for single cryptographic building blocks as well as the security of entire systems. In addition, we also touch upon legal and economic implications.

Moving on, Sect. 3 presents ways to prepare for the quantum threat. This includes explaining different approaches that exist (i.e., using "post-quantum" or "quantum" cryptography) and their differences. From that subsection on, this chapter concentrates on "post-quantum" cryptography and the "post-quantum" transition, with reasoning provided. Since a post-quantum transition might come with significant efforts and delaying the transition might pose severe security risks—both depending on the particular system—it is important to analyze preparation timeline. Tools for this analysis are explained in Sect. 3.2.

Moving forward, Sect. 4 takes a closer look at the range of factors to model and consider for systems when looking to integrate post-quantum solutions. We also cover common industry approaches to post-quantum cryptography and fallacy risks to avoid. Section 5 provides an overview of various critical and major system operations, what types of risks quantum computing may pose for such systems, and presents a risk modeling perspective.

2 The Quantum Threat and Its Implications

Quantum computers have frequently been juxtaposed with cryptography as a threat to currently deployed systems. One reason is that quantum computers have the potential to break most of the currently deployed asymmetric cryptography; however, they do not have the same devastating effect on the security of symmetric cryptography. In this section, we take a closer look at the cryptographic and broader security implications of a quantum computer, also called the "quantum threat." In particular, we first explain the implications of cryptographic algorithms using examples. We then explain how broken security guarantees of cryptographic building blocks affect the security of systems. We end this section by touching upon the legal and economic implications of the quantum threat.

2.1 Implications for Cryptography

This section explains why and how large quantum computers can break most of our currently deployed asymmetric cryptography.

As described above, for asymmetric encryption, everyone who knows the public encryption key can encrypt a message but only holders of the secret decryption key can decrypt ciphertexts (other asymmetric cryptographic algorithms work in analogous ways). That means for the encryption scheme to be secure it must not be possible to compute the secret key from the public key—yet for decryption to be possible at all, the two keys must be related. In particular, it must be easy to compute the public key from the secret key but practically impossible to compute the secret

from the public key. This can be realized using *computationally hard mathematical problems*. For example, the *integer prime factorization problem* says that given two large prime numbers it is easy to multiply them; however, given such a large product, it is *computationally hard* to compute the prime factors.

One of the most famous asymmetric encryption schemes—the RSA scheme invented by Rivest, Shamir, and Adleman [91]—is based on this construction principle. The public key is the product of two prime numbers, while the secret key is some information that enables finding the prime factors. For further details on modern cryptography, see Katz and Lindell [53]. As far as we know, no classical algorithm (i.e., algorithms run on our current transistor-based computers) solves the prime factorization problem efficiently (i.e., in polynomial time) that would allow breaking of RSA [68]. However, there exists an algorithm—Shor's quantum algorithm [95]—that solves this computational problem efficiently when running on a sufficiently large quantum computer.

Another very important computational problem that is currently a security basis for most deployed cryptographic systems is the *discrete logarithm problem* [51]. We omit the details here as for the following discussion it is sufficient to know that this problem can also be solved efficiently using Shor's quantum algorithm. We call a quantum computer *cryptographically relevant* if it is able to break instances of currently deployed cryptographic algorithms, such as RSA-2048, in a reasonable time (where "reasonable" is contingent on the application).

Interestingly, Shor's algorithm does not seem to give a computational advantage in breaking symmetric cryptographic algorithms. While another quantum algorithm, namely Grover's quantum algorithm [38], does provide a slight speed-up for attacks, it can be mitigated by essentially doubling the key length. For more details, we refer to [10].

In a surface-level assessment, this observation could be interpreted to imply that quantum resistance is realizable by simply foregoing asymmetric cryptographic techniques in favor of symmetric cryptographic algorithms throughout a system. However, as we will discuss in Sec. 4.1, such an approach is naive and introduces a multitude of risks that current systems have been made robust against. Many of those risks would be immediate—exploitable by standard adversaries without need for a quantum computer. We will discuss countermeasures in Sect. 3.1, but first take a look at the broader system security implications of the quantum threat as second- and third-order effects from breaking cryptographic algorithms.

To further compound the above risks, there is an additional approach termed *back-tracking attacks* that further magnifies the effects of an eventual attack. The back-tracking attack scenario is already taking place now—*before* large quantum computers exist. Under this attack, encrypted and authenticated communication information is captured and collected. Huge amounts of such encrypted data are then stored. Once a suitable quantum computer is available, the attacker can decrypt the stored ciphertext and the collected data becomes available and actionable to the attacker.

Notably, this approach has an added benefit to the adversary, namely through data aggregation. The concept of *classification by compilation* is common for

sensitive information [17, 50], and applies to the increased risk of disclosing sensitive information when an adversary is able to associate various data pieces and make deductions from them. Naturally, back-tracking attacks motivate transition to quantum-resistant cryptography far earlier than a quantum computer is actionable. The more data that is communicated as quantum-resistant ciphertexts, the more data stays confidential also in the future.

Moving forward, the next subsection describes how breaking the security of cryptographic algorithms impacts the guarantees of security systems.

2.2 Implications for Security

Merging from core cryptographic security into system security leads us to a wider view of integral parts and dependencies—as well as security risks and implications. System security relies on principles from the C-I-A triad, that is, confidentiality–integrity–authenticity. These system goals are applied to different system components, with varying degrees of requirements. For example, data confidentiality is essential if an adversary could collect or utilize information and authenticity ensures protections against impersonation of components. Tying together integrity and authenticity, we have that data received from a given component is authentic to the source, which avoids malicious injections.

Cryptography forms the foundation for the security of these systems as a whole. While there are numerous security measures that a system can take, those become largely irrelevant if the foundation crumbles. Under a cryptographically relevant quantum computer, the current security C-I-A guarantees no longer hold [10]. Such quantum attacks could have devastating implications for the wider system at the time of attack and thereafter. For example, consider the case of a crewed aircraft where a quantum computer is existent (a more detailed discussion on system security implications and back-tracking attacks for such cases will be covered in Sect. 5).

Figure 1 illustrates a concept of operations (CONOPS) of the aircraft from the perspective of the variety of communications links acting on the system and connecting the wider system of systems (SoS).

Failure of C-I-A security guarantees has numerous consequences in the crewed aircraft SoS. For example, among external communication links, aircraft depend on satellite systems for navigation. Attacks in real time could potentially lead to mid-air collisions or other adverse effects (back-tracking attacks could also lead to traceability for past sensitive defense missions, or forgeability of past location data to subvert auditability). Compromise of individual communication links and associated type(s) of C-I-A security have differing effects on the SoS, ranging from undesirable loss of sensitive information to catastrophic loss of the aircraft itself.

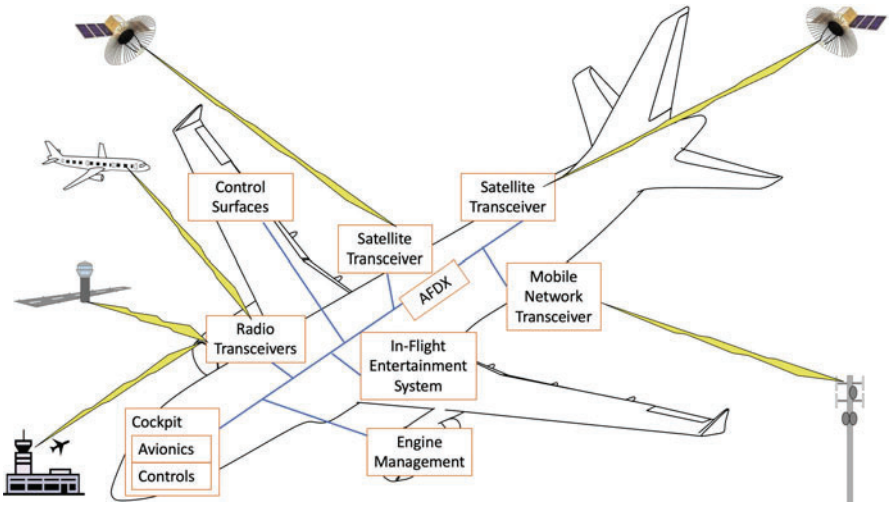

Fig. 1 Crewed aircraft internal systems. A modern crewed aircraft contains many interconnected systems that operate on internal networks such as Avionics Full-Duplex Switched Ethernet (AFDX). Several systems that may be connected to AFDX or similar networks are shown. External communications with satellites, other aircraft, and the ground are shown. Additionally, crew and passengers interact with the AFDX or similar network through avionics, control systems, and the in-flight entertainment system

2.3 Legal and Economic Implications

Security implications of a quantum computer extend past the technological threat and into the social, economic, and legal spheres. Research has analyzed how allies such as the United States, the European Union (EU), the United Kingdom, Australia, Canada, and New Zealand attempt to govern the quantum threat by studying diverse public documents, as well as how the quantum threat is perceived by the different actors [22]. Csenkey and Bindel [22] found that many public documents describe the threat as a technical threat and mention the back-tracking attack as described above. Interestingly, however, they also observed that the quantum threat is perceived as a legal issue. For example, the EU's regulatory requirements for data privacy and security might be violated by quantum attacks, creating both legal and socioeconomic implications.

In addition, it has also been found that the quantum issue is perceived as an economic threat [22] due to breaks in security, with particular risk to supply chains or business continuity. Implications from this are twofold: businesses must adapt and account for the post-quantum transition, and they may elect or be forced to shorten supply chains or find new suppliers to meet regulations if existing supply chain partners have not (yet) transitioned to post-quantum secure alternatives. This is particular important in complex systems such as the above-described ecosystem surrounding crewed aircraft.

While this chapter concentrates on the technical and system-level issues for a post-quantum transition, it should not be forgotten that the security reasons for undertaking such a transition have repercussions at various levels of society. Cybersecurity underpins much of the digital and larger cyber-domain today, and even seemingly unrelated operations with any fringe connection using software, hardware, the Internet, or radio frequency transmissions are liable to be impacted. Thus, the impact of disregarding the quantum threat goes well beyond technical implications and might threaten almost all aspects of our daily lives, economy, and society.

To conclude this section, quantum computing presents a risk to asymmetric cryptography—a core foundation to many systems today. Thus, by implication, quantum computing poses a significant risk to wider systems. Such security risks have third-order effects on auditability, civil rights, and even supply chain integrity, leading to an urgency for action in support of legal and economic functions that may be seemingly far removed from cybersecurity considerations. In the next section, we will take a closer look at cryptographic tools and preparation timelines.

3 Preparing for the Quantum Threat

Inventing (or even standardizing) alternative quantum-secure cryptography is just the first of many steps required to prepare for the quantum threat. Consequently, in this section, we look at not only basic quantum resistant cryptographic solutions but other factors and timeline implications of a transition to post-quantum cryptography.

3.1 Post-Quantum Cryptography vs. Quantum Cryptography

Currently, there are two main cryptographic directions that use the term "quantum": post-quantum cryptography and quantum cryptography. Naturally such similarity in terms can lead to confusion, with potential consequences in procurement of system solutions that may not solve the intended security problem.

The first approach, quantum resistant or *post-quantum (PQ)* cryptography, is designed for the explicit goal of defense from a quantum adversary.[1] Collectively, such techniques are called *post-quantum cryptography (PQC)*, and in particular algorithms are called, for example, post-quantum digital signatures, post-quantum public-key encryption algorithms, etc. Researchers, industry, and standardization bodies have been working on post-quantum secure alternatives for more than 15

[1] Early schemes such as the code-based McEliece and the lattice-based NTRU encryption scheme that have been designed in the 1970s and 1990s, respectively, have not explicitly been designed to resist quantum adversaries.

years. In 2017, NIST started standardization of post-quantum public-key encryption and digital signature algorithms [2].

This approach enables use of current public-key infrastructure and relies on switching out the cryptographic algorithms being used. In a more concrete example, a quantum-vulnerable algorithm like RSA must be substituted with post-quantum algorithms. Post-quantum algorithms are based on different mathematical construction principles that are not known to be efficiently solvable by quantum algorithms. Post-quantum secure algorithms are constructed over different computationally hard problems than quantum-vulnerable algorithms. Thus, new algorithms are not vulnerable to Shor's quantum algorithm. Much research has been done on the selected computationally hard problems [9, 33, 76] as new alternatives to the prior selections.

Notably, post-quantum cryptography is designed to be run on current transistor-based computers. Hence, no physical changes have to be made to the infrastructure. It does not require any special (i.e., quantum) equipment to protect against the threat. However, post-quantum algorithms do come with different performance metrics (algorithm efficiency and memory requirement) than currently used algorithms. Therefore, some adjustments within the current infrastructure have to be made. This can be as little as increasing the allowed sizes for public keys, ciphertexts, or digital signatures in software implementations. If a current system is under strict limitations, however, such a transition might also mean that hardware needs to be exchanged to allow for more space. We will elaborate on this topic in Sect. 4.4.

The second direction, *quantum cryptography*, also covers "quantum key exchange" or "quantum key distribution" (QKD). This technology uses principles of quantum physics similarly to but differently from quantum computers described in Sect. 1 in that it looks to use quantum computing for potentially interesting cryptographic advancements. It differs from post-quantum cryptography in that instead of being designed with the intention of protecting against a quantum adversary/quantum computer, it explicitly aims to apply quantum computing principles to creating new cryptographic techniques. Thus, quantum cryptography may, but also may not protect against a quantum adversary, as described in more detail below. In QKD, sent and received quantum states are essentially the "secret keys" that are then used to encrypt data using symmetric encryption. By the laws of physics, keys that have been eavesdropped on by attackers will not be received correctly anymore, thus implying that, if parties end up with the same key, an eavesdropper was not active.

While not designed to specifically counter a quantum threat, the design of QKD using quantum states makes it naturally resistant to the types of quantum attacks discussed earlier. Thus, QKD has also entered the space of terms referred to when looking at security against a quantum attacker. However, there is a subtle yet significant security gap to such claims that is often evaded when QKD is marketed as a solution to the quantum threat. Namely, QKD does not solve *entity authentication*. Colloquially, entity authentication is assurance that the party sending data is who they claim to be. Thus *data authenticity*, *data confidentiality*, and *key secrecy* are all reliant on first achieving entity authenticity—to show that data is confidential

to two parties, not manipulated, etc., one must first know that the other party is not impersonated. QKD does not solve entity authentication and is therefore reliant on classical methods of authentication. For example, geo-location of the intended communication partner must be both pre-established and so precise that it is impossible that another entity can impersonate them, or a cryptographic method for entity authentication must be used. Without such an added entity authentication solution, an attacker can impersonate communication partners or perform man-in-the-middle attacks. Cryptographic methods for entity authentication rely on one of two approaches: (1) a symmetric key or (2) an asymmetric key. In both cases, QKD relies on assumptions similarly to post-quantum algorithms.

In addition to the above considerations, QKD comes at the cost of physically building a new infrastructure that physically connects or provides line of sight between the end points. Moreover, state-of-the-art QKD systems either have a rather short range (approximately 100 km [7] with some experimental results extending to longer ranges [77]) or require "repeaters" to help relay the communication over longer distances. Unfortunately, such repeaters have a history of being vulnerable to attacks, casting an additional security concern for QKD in practice [7, 100]. Therefore, QKD seems to serve as a solution for certain applications, but not as a general protection suitable for all of tomorrow's diverse security needs.

In the remainder of the chapter, we focus primarily on post-quantum algorithms vis-a-vis quantum cryptography, QKD, designing quantum computers, or quantum technology in general as we concentrate on transition strategies and challenges for hardening against a quantum threat. Notably strategies and challenges for use of quantum computing differ significantly from defense against such adversaries.

3.2 Post-Quantum Transition Timeline

The immense efforts in developing post-quantum alternatives have constituted a significant step in securing systems against a quantum attacker. However, as NIST itself states, "…it appears that a transition to post-quantum cryptography will not be simple as there is unlikely to be a simple 'drop-in' replacement for our current public-key cryptographic algorithms" (NIST, Call for submissions, 2017 [20]). This statement implies that, while NIST is standardizing foundational algorithms, that is merely the beginning of the transition. Further context must be accounted for *in addition to* use of post-quantum algorithms.

Combining development with back-tracking attacks, Mosca [65] illustrates the urgency of a post-quantum transition with a simple equation:

$$l + d > q,$$

where l gives the lifespan of the information that needs to be kept secret, d is the number of years needed to deploy post-quantum algorithms in the respective applications, and q corresponds to the number of years until cryptographically

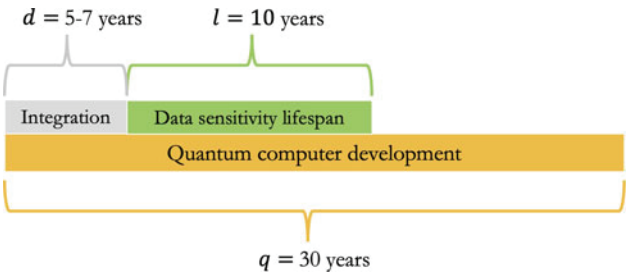

Fig. 2 Illustrated example of data sensitivity lifespan (green), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow). In the illustrated example, data sensitivity lifespan is relatively short compared to the development timeline for a quantum computer. In practice, it is unclear how many years duration can be assumed for the yellow timeline

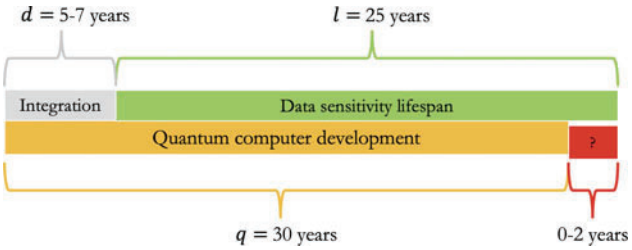

Fig. 3 Illustrated example of data sensitivity lifespan (green), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow). In the illustrated example, data sensitivity lifespan implies that several years of data would be vulnerable (red) in the event of a quantum attack. Moreover, if back-tracking attacks are accounted for, all data in this illustration is vulnerable (the yellow component would need to be longer than the combined gray and green components to avoid such attacks). If the development timeline of a relevant quantum computer was less than 30 years, the amount of compromised information would be even greater

relevant quantum computers can be built. We visualize this using an example in Fig. 2.

In the illustrated example, system risk is low given an assume quantum computer development timeline of $q = 30$ years; under such an estimate, there would be sufficient lead time to plan for and integrate post-quantum cryptographic measures. However, the image oversimplifies the situation. Not only may an estimate of 30 years for development of a quantum computer be overgenerous, but the data sensitivity lifespans in some systems are well beyond 10 years. For the illustrated example in Fig. 3, if data sensitivity is, for example, 25 years, then even an assumption of a 30-year development timeline for a quantum computer is insufficient to protect data.

Mosca's equation can be applied to calculate the urgency to start the post-quantum transition for an entire system's public-key infrastructure, but it can also be used for estimations for specific applications. For the latter use-case, we would extend the equation by yet another variable, h, representing the lifespan used in the

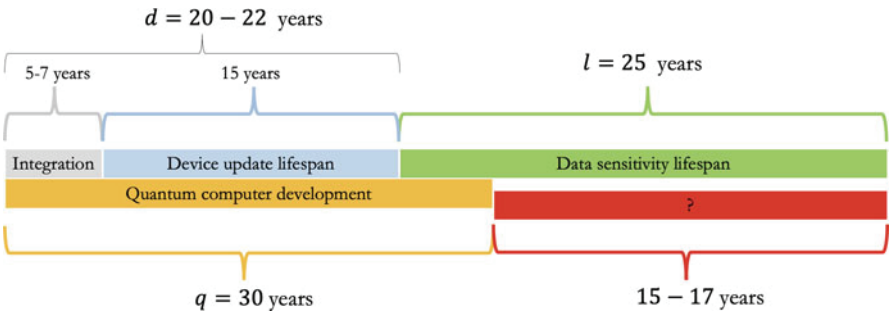

Fig. 4 Illustrated example of data sensitivity lifespan (green), device lifespan as a function of the update frequency for internal cryptographic algorithms (blue), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow). In the illustrated example, consideration of update potential significantly increases the data-at-risk lifespan, and even without back-tracking attacks decades of data would be vulnerable in the event of a cryptographically relevant quantum computer. To protect against back-tracking attacks, the cumulative end of the gray/blue/green timelines would need to be earlier than the yellow quantum computer development timeline

device-to-be-transitioned. For example, if a cryptographic algorithm is implemented in hardware on a device and that device is then deployed in practical use, h could represent an extended period of time. If the algorithms are implemented in software, then updates may be more frequent; however, on the user end of the spectrum, smart yet "disposable" Internet of Things devices may never receive a manufacturer software update. In either of these cases, the available cryptographic algorithms are tied to actual device lifespan. If cryptographic algorithms were programmed in hardware for a system used in outer space, for example, that system may perform its entire intended functional purpose—lasting years—without an update to the cryptographic algorithms used.

Figure 4 illustrates a case such as described above, where a device has an extended lifespan of 15 years due to, for example, programming in hardware and the deployed device being inaccessible for updates (such as deployed in space). Due to an added 25-year data sensitivity lifespan and the risk of back-tracking attacks, post-quantum algorithms are employed. Thus, not only must the post-quantum algorithms required be developed prior to device deployment, but protocol development and integration must also take place (see Sect. 4). It is not possible to "drop-in" solutions without accounting for functional needs due to both the differences in post-quantum algorithm memory/computational cycle costs and potential needs for post-quantum protocols vs. algorithms. In this example, we see the quickly accrued time: a minimum of 45 years in the example. It is unclear when a cryptographically relevant quantum computer will be actionable; however, the entity responsible for a system would, in this example, either need to be confident that such a quantum computer is not actionable for 45–47 years, or assume all risk for the potentially substantial "red box" time period.

Cryptographic agility plays a notable role in the implications of the additional "blue" timelines in these figures. A system that is capable of regular updates will more nearly approximate Fig. 3. In fact, for many working in the cybersecurity sector who maintain full system control and are able to readily replace system components, the timeline shown in Fig. 4 may seem protracted; however, for various systems in government infrastructure, critical systems, defense sectors, and irregular environments (e.g., undersea, polar, and outer space), various components may be either hard to reach or were never intended to be replaced until the entire device expires. As such, systems being fielded now, even before post-quantum integration, should be carefully considered for cryptographic agility and the ability either to update the algorithms or retire the entire device if needed, to ensure that the "blue" device lifespan is minimized.

Figure 4 is illustrated as a single "device" with lifespan in blue; however, a typical system will include a multitude of components, some of which the system manager does not have an option to introduce post-quantum solutions to at a later date (e.g., commercial-off-the-shelf (COTS) devices with algorithms implemented in hardware). Within a system, the weakest link is a prime target for a cyberattack, and system information may be generated, shared, and acted upon by various components. Individual systems will vary, but a general guideline for a system's *pre-quantum lifespan* is the longest common duration across all components. Even if most components are updated at a moderate frequency, the quantum risk to the entire system should thus be gauged on the weakest component, as illustrated in Fig. 5. For example, an aircraft may rely on several communication links with different control components—for example, Global Positioning Systems (GPS),

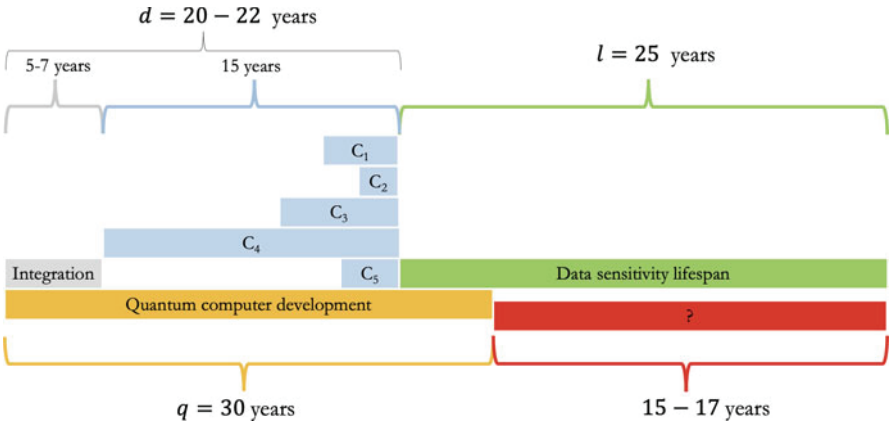

Fig. 5 Illustrated example of data sensitivity lifespan (green), device lifespan as a function of the update frequency for internal cryptographic algorithms (blue), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow). C_i indicates the i-th component. In the illustration, there are five components in the system, with the pre-quantum lifespan of the system being dependent on the longest common component lifespan duration (here C_4)

radio communications, and ISR relays—each with a different manufacturer, and all contributing to the aircraft command and control. Each component may be on a different update schedule from its provider and require different types or degrees of quantum resistance. However, the entire aircraft is only quantum-resistant in its operation if all components are. Thus, if one aircraft component is quantum-vulnerable but is rarely updated or impossible to update without a major replacement cost due to legacy design, then that component contributes to a quantum-vulnerability for the whole system, regardless of whether or not other components are updated. Therefore, it is important to analyze the urgency of the post-quantum transition for smaller compartments as well as the entire systems to accurately estimate the time needed to deploy post-quantum algorithms to the entire system.

For more customized and protracted device designs, such as may be necessary for sensors in nuclear energy systems, proprietary system components, and other nonagile system components, this may prove to be an even greater risk due to procurement life cycles. For example, if a satellite system component is custom-made on a competitive contract for a government entity, then not only do the design, integration, and component lifespans factor into d, but the acquisition process timeline must also be accounted for. Figure 6 illustrates this consideration.

In conclusion of this section, it is important to emphasize that the point of time when to start to transition to post-quantum secure cryptography is not trivial. This holds in particular for large systems as these are only as secure as their weakest building block. Moving on, considerations during the post-quantum transition are discussed.

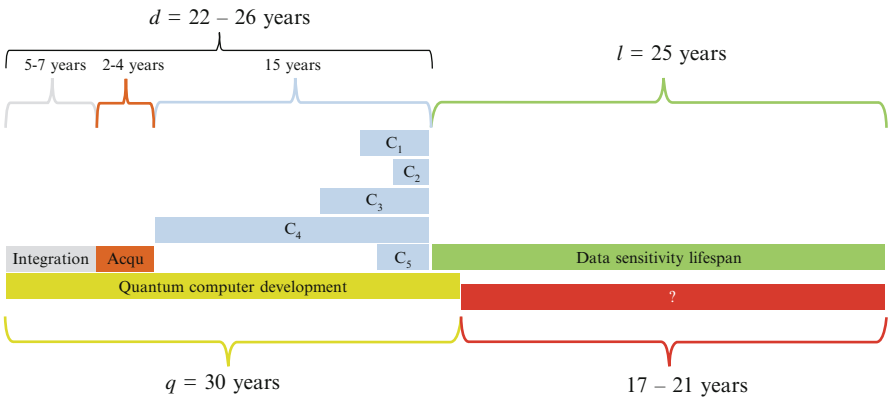

Fig. 6 Illustrated example of data sensitivity lifespan (green), device lifespan as a function of the update frequency for internal cryptographic algorithms (blue), acquisition process timeline (orange), post-quantum integration time (gray), and a potential cryptographically relevant quantum computer development timeline (yellow). C_i indicates the ith component

4 Post-Quantum Transition: Integration Considerations

Industry has taken action in response to the urgency of the quantum threat, and governments and defense sectors have begun to look at post-quantum options [22]. With many options available and various terminologies in use, a natural question for system designers is how to sort information and what considerations should drive decision-making regarding the post-quantum transition. In this section, we provide a cautionary note to the reader about certain technology categories advertised for quantum resistance and then turn our attention to example transition considerations for decision-makers to use when assessing system needs and options.

4.1 A Cautionary Note

Various companies have established new business models on offering post-quantum cryptographic solutions and more established companies have also added post-quantum cryptography to their offered services, capabilities, or features [1, 5, 47, 49, 52, 55, 59, 78–89, 103]. Distinguishing among such solutions and the appropriateness of them could be a challenge to system management. Furthermore, there is also the potential for "snake-oil" solutions to be marketed among actionable options, creating yet a more complex array to sort through. We provide a cautionary note on two types of claimed solution sets that may either not be generically appropriate or that may introduce unnecessary complexity to a system without coherent security gains. While it is not impossible that an appropriate solution could occur within one category or the other, system maintainers should carefully assess their threat model and needs before considering these.

Symmetric Techniques

Symmetric key cryptography has been in existence for centuries, with the Roman Caesar cipher being an early example. Thus, symmetric techniques have long predated the introduction of the asymmetric cryptographic techniques now threatened by quantum computing. Moreover, symmetric cryptographic techniques do not use the same underlying designs that make many current asymmetric cryptographic algorithms susceptible to quantum attacks; hence, currently, it seems that entire symmetric algorithms do not need to be replaced but rather only the key sizes used in them increased [61]. Therefore, it might seem tempting to resort back to systems relying only on symmetric cryptography. In what follows, we caution against this approach as it does come with downsides.

Since there is no means in a symmetric key protocol for two parties to establish a key using only public information, symmetric keys must either be pre-distributed or distributed by a trusted third party. This raises the question: *What third-party*

should be trusted with knowledge of keys and therefore transmitted information? The security considerations are many; even if the third party is a vetted access entity, for example, a key distribution hub internal to a government entity, the nature of such a hub makes it also a high-value target and a single point of failure. If an adversary was ever able to gain access/hack-in/etc., they would also gain access to not one communication link's data, but an entire system of data in a single strike. Coupled with back-tracking attacks, such a third-party approach could be even higher risk if keys also are not changed frequently (providing a form of *forward secrecy*). Thus, even a vetted and self-contained third-party key management for symmetric keys not only lacks defense-in-depth, but is actually far weaker than most current cryptographic key infrastructures. When the third party is an external software provider, then not only does all the above apply, but there is an added risk stemming from that entity's access to the keys and consequently the potentially sensitive data being transmitted, for example, in a government or defense system.

Given the above, it may seem odd that some systems still use symmetric key management infrastructures. To understand this, we can examine an example of a common, modern protocol that still relies on symmetric key cryptography—the Kerberos protocol [72]. Kerberos is used, for example, in Microsoft Windows [104], which employs a Microsoft component as a trusted third party to provide keys to other Microsoft components. In Windows, Kerberos is used for example to support user single sign-on to allow access to a variety of Microsoft services. Thus, we see an equal-trust paradigm in this use of Kerberos; if a user is acting on their own (e.g., a laptop is accessing all Microsoft components within the laptop under their physical control), then trust in another Microsoft component to help manage that access does not substantially change the access risk. Thus, the choice of this symmetric key management and security thereof is highly dependent on the needs and security assumptions of the use-case.

When investigating potential post-quantum system solutions, it is thus advisable to be cautious of solutions that advertise quantum resistance but eschew use of public-key algorithms altogether. Such solutions may in fact evade the process of replacing current asymmetric cryptographic algorithms with post-quantum cryptographic alternatives by instead resorting to symmetric-only designs and "downgrading" system security to highly vulnerable trust infrastructures.

Mixing Quantum and Post-Quantum

Another aspect worthy of caution is conflation of security properties offered by quantum cryptography with those of post-quantum cryptography. Section 3.1 discussed the intent of quantum cryptography and gaps in application to problems of quantum resistance. Notably, quantum and post-quantum cryptography describe two very different subfields of research and are even designed with different fundamental requirements (i.e., post-quantum cryptography can run on a classic computer whereas quantum cryptography is designed for a computer supporting quantum

mechanics). Thus, solutions claiming a mixture of these terms and guarantees should be considered with caution.

Ultimately, when a system maintainer selects a solution it should be based on the particular system's needs—both in terms of security and threats. Failure to do this can lead to use of solutions that cause unnecessary computational cost, memory cost, physical space and weight, or even simply product cost. In this context, and considering the mixed goals and design requirements of post-quantum cryptography and quantum cryptography, managers should carefully assess whether such a solution provides their particular system any security benefits over a more streamlined post-quantum solution.

4.2 Confidentiality vs. Authenticity

As mentioned earlier in the chapter, *confidentiality* and *authenticity* are two of the core security guarantees that cryptography can provide. Section 3 looked at data lifespan as a consideration factor for post-quantum transition, and we can take a closer view at the implications for each of these two guarantees under a quantum threat. Each guarantee may have a different sensitivity lifespan and each is dependent on the use-case, hence it is critical to assess system goals when undertaking a post-quantum transition.

Confidentiality is the guarantee that an adversary cannot *read* or *eavesdrop* on transmitted data. Whether such data is sensitive mission data, proprietary information, critical infrastructure planning data or daily monitoring levels, or even simply email contents, each type of information has a different lifespan. Sensor data, for example, temperature readings, may have a relatively short lifespan. If an adversary was to learn thermostat readings in 10 years then, even with a back-tracking attack, the information may not be particularly useful. If the lifespan is short, then there is more leeway time for post-quantum integration (at least for algorithms and protocols affecting confidentiality). In contrast, the criticality of an early post-quantum transition for, for example, classified information transition may be higher. Government, legal, and other higher-profile systems regularly handle sensitive information of a longer lifespan or data that, if decrypted even several years later, could be aggregated for malicious effects. Such data can, for example, have a 25-year lifespan [45], with back-tracking attacks based on this lifespan shown in Sect. 3.

There is also a middle ground of information sensitivity. For example, the 2014 hack on Sony Pictures released emails, information on planned films, personal data, and salary information [39]. Suppose that such a hack took place using a quantum computer, for example, 10 years after the emails, personal information, and information on planned films was sent and that the adversary employed a back-tracking attack to decrypt all the data. Perhaps 10 years after the fact a planned film would already be made, thus expiring the sensitivity of the information. However, personal information would still be actionable. Moreover, email content could

expose the company to lawsuits and salary information could make individuals financial targets. If that hack was 5 years or 15 years after time-of-send, the sensitivity of each of these data types might range from expired to very sensitive. In short, the type of information sent across a communication channel and potential malicious uses of it must be weighed to identify the urgency of post-quantum need for that channel or use-case.

In contrast to confidentiality, *authenticity* is a term usually applied to two aspects within cryptography: *data authenticity*, which is also often referred to as *integrity*, and *entity authenticity*.

Data authenticity, a.k.a. *integrity*, refers to a malicious actor's ability to modify, forge, or otherwise manipulate data. Digital signatures (asymmetric algorithms vulnerable to a quantum adversary) are often used in, for example, S/MIME email signatures as well as web connections and even credit card payments (see [24, 69] for a good overview). In terms of lifespan, a quantum adversary that is able to break a signature key in the future and retroactively forge a transaction or web connection that occurred several years prior may have little gains; thus, in many cases, people argue that post-quantum transition of data authentication algorithms is less important than encryption. However, such arguments depend on the perspective. For example, a user may not be concerned about forgery of grocery receipts when a payment card is already expired, but the legal system's reliance on such digital proofs against forgery takes on higher risks.

Consider, for example, a land ownership document that is digitally signed, for example, through DocuSign [99]. If an adversary was able to break a digital signature on the land deed years after transfer of property, they may successfully create a case to contest ownership—or to argue ownership by multiple entities. Similarly, the legal implications of signing contracts and various government documents rely heavily on the unforgeability of such documents long into the future. To use other terms, a quantum adversary using back-tracking attacks could subvert auditability or nullify the validity of audits. Thus, data authenticity must also be considered relative to the use-case needs and the required auditability lifespan, for example, matching the green box in Fig. 4.

Entity authenticity refers to protections against impersonation ("forgery of identity") vice data forgery. For example, when connecting to an online bank, a user wants to have a guarantee of the legitimacy of the bank's website in order to avoid identity theft and the bank wants to have a guarantee of the user's identity, to avoid liability of impersonation to access funds. Frequently, this is seen as a much shorter "lifespan" interaction—if a viable quantum computer against the cryptographic aspects becomes a reality (e.g., 10 years after a banking log-on), the risk to that transaction is minimal. Entity authentication, however, is also tied to data authenticity, in that forgery of the entity calls into question validity of the data. In many cases, identities are tied to a *Public Key Infrastructure (PKI)*. Under PKI, some trusted third-party certificate authority uses digital signatures to sign off on certificates to link an identity to a public key. Thus, if the authority's key itself is obtained by a quantum adversary, that adversary can impersonate various identities as well as forge data by them. Again, if we are assuming back-tracking

attacks for some future quantum adversary, then these forgeries are "after the fact." Nonetheless, the scale of damage that an adversary may achieve in terms of legal and audit validity effects is many orders of magnitude larger when they are able to attack the third-party certificate authority in contrast to only one end-user. A natural solution to this problem may appear in the form of transitioning the certificate to using a post-quantum algorithm—even if the end-user digital signature is standard, then at least it is not possible for an eventual quantum adversary to retroactively create competing identities. Unfortunately, this solution is inhibited in that current systems must be able to validate the certificate authority's signature on a certificate; therefore, ironically, the certificate authority's algorithm may be the last to be upgraded as legacy systems need to recognize it. Thus, we see that there is a larger infrastructure around achieving post-quantum data authenticity that takes time to transition, creating an urgency to do so that may not be immediately apparent. In Sect. 4.5, we will discuss post-quantum *hybrid* techniques that may help solve the legacy challenge.

4.3 Protocols vs. Algorithms

In cryptography, protocols and algorithms are interdependent but separate concepts. For example, encryption is a cryptographic algorithm—a function—than, on input of keys and data, provides a ciphertext output. An example of a cryptographic protocol includes key exchange protocols—interactive steps between parties for establishing the key that is then used for encryption. Other examples include mutual authentication protocols such that parties are protected against impersonation within the channel, consensus protocols, and privacy-preserving protocols, to name a few. In the case of data encryption, the security of the encryption algorithm is directly reliant on the security of the key exchange protocol used to establish the encryption key. If the latter breaks and an adversary could obtain the key, then it will also be able to decrypt information that it should not have access to. Protocols are used in most aspects of daily life, including to secure digital communications to banks, smart door locks, car keys, pacemakers, among Internet of Things devices, etc. This raises a question: when identifying quantum resistance measures for system hardening, should post-quantum secure techniques be applied to the algorithm, the protocol, or both?

Security of even the most simplistic of systems relies on cryptographic protocols to combine algorithms in dependable and resilient ways. Algorithms can be used as "building blocks" for secure protocols. For example, version 1.3 of the Transport Layer Security (TLS) protocol combines cryptographic key derivation functions, message authentication codes, and digital signatures, among others. Even if the underlying components are strong, they could be combined in such a way that the resulting protocol is broken and the adversary learns the secret information. Thus, having post-quantum algorithm subcomponents is necessary for the post-quantum security of the protocol, but not sufficient to automatically imply that the overall

protocol is secure, and analysis of the protocol itself must be considered. Finally, protocol security is dependent on the threat model of the system (i.e., what it is trying to protect against) and this frequently extends to many other threats than just quantum computing. Some protocols are being created or adapted that may be suitable for post-quantum applications [15, 16, 21, 26]. Other protocols that are already tailored for efficient and secure use inside of a given system may require a re-tailoring with post-quantum algorithm subcomponents to assess suitability against both a quantum attacker and the system's current core threat model.

In summary, the answer to the above question is that it is not sufficient to simply replace quantum-vulnerable cryptographic algorithms—the entire protocol needs to be analyzed and potentially changed to achieve overall protection against quantum adversaries.

4.4 Software vs. Hardware

As explained in Sect. 3, the number of years needed to deploy a system is determined by the time of integration, the acquisition process, and the device lifespan, at a minimum. The latter two are particularly important if hardware needs to be replaced. For example, for communication between aircraft or vehicles, messages are authenticated using digital signatures and then broadcast (see Sect. 5.2 for a detailed description of aircraft communication systems and [48] for a current vehicle-to-vehicle communication standard). In high-traffic areas, this means that aircraft or vehicles might need to verify hundreds of signatures. Hence, dedicated hardware chips that implement the verification algorithm are often integrated in the aircraft or vehicles to improve efficiency over software implementations. During a post-quantum transition, post-quantum algorithms must first be implemented and tested for the needed hardware processors, and then these dedicated chips must be manufactured and deployed in systems. There are a few works on how to reuse dedicated hardware chips for classical algorithms for a post-quantum algorithm. For example, [3] describes how to reuse RSA processors for transition to the lattice-based scheme Kyber. However, whether this is possible depends very much on the hardware as well as on the specific cryptographic algorithms being used.

This means that if a system includes dedicated hardware implementations for cryptography algorithms, the urgency to analyze the system regarding the need for a post-quantum transition is increased. Urgency also increases with the scale of the application. For example, while replacing one Automated Teller Machine (ATM) with an ATM that has been upgraded to be post-quantum secure may be a relatively feasible process, replacing all 470,135 ATMs in the United States. [4] requires an immense effort both in timescale management and financial investment.

In contrast, upgrading software is presumably easier as in most cases no hardware changes need to be made. However, the effort arising from potentially many dependencies in software libraries should not be underestimated. Further, many different companies make ATMs that may require many different software upgrades to transition all ATMs to post-quantum security options.

4.5 Classical/Post-Quantum Hybrid Algorithms

The urgency to switch to post-quantum secure cryptographic alternatives that has been described in this section is opposed by the uncertainty of whether post-quantum algorithms are secure. Cryptographic algorithms are naturally a high-value target for attackers due to the information advantage, with second-order effects from breaking an algorithm including financial and strategic impacts. Thus, cryptographic algorithms, whether classic or post-quantum, receive an intense degree of scrutiny, cycling through phases of uncertainty, breaks, and hardening revisions. Among the NIST post-quantum candidates, some algorithms have a fairly long history of testing, such as hash-based signature schemes (e.g., XMSS [44]), which are already recommended by the German Federal Office for Information Security [32], or the code-based Key Encapsulation Mechanism (KEM) McEliece [8]. The security of these is therefore more thoroughly vetted than some of the newer alternatives that are also up for standardization. For example, Rainbow [25] is a post-quantum algorithm invented in 2004 that has made it through three rounds of the NIST post-quantum standardization effort. Nonetheless, in 2022 research emerged that demonstrated significant vulnerabilities in Rainbow [11, 27], leading to key recovery attacks.

While it may be enticing to forgo newer algorithms in favor of those with more history to increase the likelihood of sudden security breaks, there is no guarantee that such time maturation provides indication of security—historically ciphers that have been thoroughly cryptanalyzed for many years have also been identified as holding new vulnerabilities [14, 68]. Second, newer algorithms can provide different features than some of the more established variants. In post-quantum cryptography, there are usually trade-offs in memory or computational requirements, and for some applications the current algorithms possessing a longer history may not be suitable. Finally, the urgency for a post-quantum transition may prohibit a longer waiting period for more results to emerge.

As a solution to this predicament, hybrid or composite algorithms [12, 13, 75, 96] have been suggested that have also been recommended by standardization agencies such as NIST [18], the German BSI [32], European Telecommunications Standards Institute (ETSI) [28], and the Internet Engineering Task Force (IETF) [23]. *Hybrids* refer to the combination of two or more algorithms of the same kind. For example, a *hybrid digital signature* may consist of a combination of two underlying digital signatures. Hybrids can be achieved by either combining classical (i.e., quantum-vulnerable) with post-quantum secure algorithms or combining different post-quantum algorithms of the same kind. The former approach aims to leverage security guarantees from classic algorithms that are well-understood but quantum-vulnerable while combining those with post-quantum guarantees. Such hybrid algorithms are post-quantum secure (if analyzed for that goal) and may also support backwards compatibility in some cases (e.g., a system that is not set up to verify the post-quantum component may still verify the classic component). In contrast, the latter approach of hybridizing two post-quantum algorithms aims to decrease the likelihood of a successful attack by spreading security across different types

of assumptions (e.g., digital signatures designed based on different computational hardness assumptions).

As with selecting whether to post-quantum transition individual algorithms (e.g., encryption, digital signatures, etc.) and protocols based on system security requirements, the use-case needs should be assessed when considering use of hybrids. Hybrids do generally come at a higher performance cost, so use may be best as a stop-gap solution during post-quantum transition or where the potential security benefits outweigh the overhead. Thus, it may be important for a system to have, for example, a hybrid key encapsulation mechanism to ensure extra security for the key distribution both under a classic and quantum adversary while only requiring, for example, a classic digital signature. Generalization of such system requirements would be ill-advised and instead the transition strategy should account for individual system use and security guarantees required.

4.6 Considerations Summary

In summary, the following considerations are important when analyzing whether or not—and when—a post-quantum transition for a system is necessary.

The first and most important question to ask is whether the system might be vulnerable to a quantum attack. This can be analyzed by answering the following question formulated by Mosca and Mulholland [63]: "Does my [system] rely on asymmetric cryptography to encrypt information, provide data integrity, or for cryptographic key distribution?" If the answer is no, no further action is needed. If the answer is yes, the next important step is to analyze the urgency of the needed transition.

As we explained in detail above, the urgency is defined by the data sensitivity lifespan—how long the communicated data needs to be secure—and the number of years needed to deploy quantum-secure alternatives. The latter can be further determined by considering the integration time, the acquisition time (of, e.g., requisite hardware), and the device lifespan of the devices used in the system. All three of these depend, on the one hand, on how crypto-agile, and therefore on how easy to change, the system's building blocks already are. On the other hand, they also depend on whether the system update would include changing hardware or only software (see Sect. 4.4). To analyze the data sensitivity lifespan, in particular two security goals need to be considered: how long does the data need to be confidential and/or how long does the data need to be authenticated (see Sect. 4.2).

In addition to determining the urgency of the needed transition, an important question to answer is also whether the quantum-vulnerable algorithms should be switched by post-quantum algorithms or by (classical/post-quantum) hybrid algorithms (see Sect. 4.5). Reasons to do the latter could be, for example, to diversify security risks (i.e., to avoid a sudden break of a single algorithm) or to enable backward compatibility with post-quantum unaware parts of the system. It is important to emphasize that not only might replacement of quantum-vulnerable

algorithms with quantum-secure algorithms be needed, but additional changes to the protocol or system as a combination of such algorithms might also be essential (see Sect. 4.3).

5 Case Studies in Quantum Risk and Transition for Critical Systems

Many systems critical to modern life require cryptography to safely and securely operate. For instance, critical infrastructure such as the power grid, water utilities, healthcare systems, transportation infrastructure including the physical built infrastructure, ground vehicles, ships, aircraft, defense systems, and many other such systems and SoS heavily rely on keeping data secure [66]. Eavesdropping on command and control (C2) and ISR data from UASs used as part of national defense could allow for an adversary to gather sensitive intelligence data that puts a nation's security at risk. This includes eavesdropping on encrypted data traffic and performing a back-tracking attack years later by quantum adversaries as described in Sect. 2.1.

This section discusses the potential risks to critical systems in a quantum-computing era through the lens of some example analyses to understand when post-quantum upgrades and overhauls to existing and future systems must occur. More concretely, we consider case studies in medical devices, satellite systems, aircraft SoS, and finally nuclear power plants.

It is important to note that while there is strong advocacy that the analysis shown in Sect. 3 should be conducted, that analysis is explicitly excluded below. The reason is that the data necessary to conduct the analysis across the examples shown in this section is generally proprietary and confidential in nature, and resides with companies that manufacture the systems discussed. In some examples, the relative urgency is discussed for a system to implement post-quantum cryptographic solutions but this is only general information and in practice may be different for specific systems of concern.

5.1 Medical Systems

As noted analogously for the cryptographic layer, system implications of a quantum attacker vary across system designs, data lifespan, and data sensitivity. Many types of data a system may have are only relevant for a brief period of time such as throttle position data transmitted across a vehicle's controller area network (CAN) bus. Other types of data such as ISR data collected by a defense system may be sensitive for many years. Further, as discussed in Sect. 2, data aggregation can lead to back-tracking attacks.

An example of a continuous positive airway pressure (CPAP) machine demonstrates data sensitivity lifespan of the hardware. CPAPs are often expected to last three to five years of nightly use by patients at home. A typical development cycle for a new generation of CPAP machine can take several years and may reuse significant system elements from previous CPAP generations. Corresponding to Fig. 6, the lifespan of data is $l = 50$ years under, for example, the old U.S. Health Insurance Portability and Accountability Act (HIPAA) (and now indefinite) [29]. Moreover, the deployment time d must additionally account for reused system elements, integration, and acquisition such that the data is post-quantum safe in the event of a quantum attacker. Note that even under an unrealistic but ideal scenario of $d = 0$, the fact that $l = 50$ or more years necessarily puts intense pressure on medical providers. If a cryptographically relevant quantum computer is viable in $q < 50$ years, then providers not using post-quantum secure options today would be in violation of HIPAA compliance for current data, given the reality of back-tracking attacks.

5.2 Aircraft System of Systems

A crewed aircraft SoS is comprised of ground control (air traffic control, airport ramps, maintenance facilities, airline logistics and management, etc.), two-way audio and digital communications (direct digital and analog radio communications and digital radio communications via satellite relay), anticollision systems (traffic collision avoidance system, ground proximity warning system, automatic Dependent Surveillance–Broadcast system, etc.), the crew (pilot, co-pilot, etc.), passengers and associated systems (i.e., in-flight entertainment system), and the aircraft itself (avionics, engines, fuel management system, control surfaces, etc.) [64]. As such the crewed aircraft SoS contains many digital systems to communicate with the ground, to other aircraft, to internal aircraft systems, among the crew, and to entertain the passengers. Many of the digital systems aboard the aircraft are linked via a data bus (ARINC 429, AFDX, MIL-STD-1553, etc. [35]). Some passenger-accessible systems such as the in-flight entertainment systems could be attack vectors to sensitive aircraft systems [30, 107]. When modern, "smart" aircraft supporting Wi-Fi are considered, we can look at WPA3—the latest of the Wi-Fi connection standards. WPA3 relies on asymmetric techniques within the Dragonfly handshake [41, 46, 102], making it vulnerable to quantum attacks. Transitioning such systems to use post-quantum techniques would be a longer process since transition for aircraft components must be accounted for in addition to any upgrades of the supported standards outside of the aircraft environment [64, 93]. On the ground, aircraft often digitally interface with maintenance equipment to run diagnostics, download prognostics and health management data from major aircraft subsystems, and upload data to the aircraft such as navigation information and updates to critical flight systems [94]. Figure 7 provides a simplified CONOPS of the aircraft SoS.

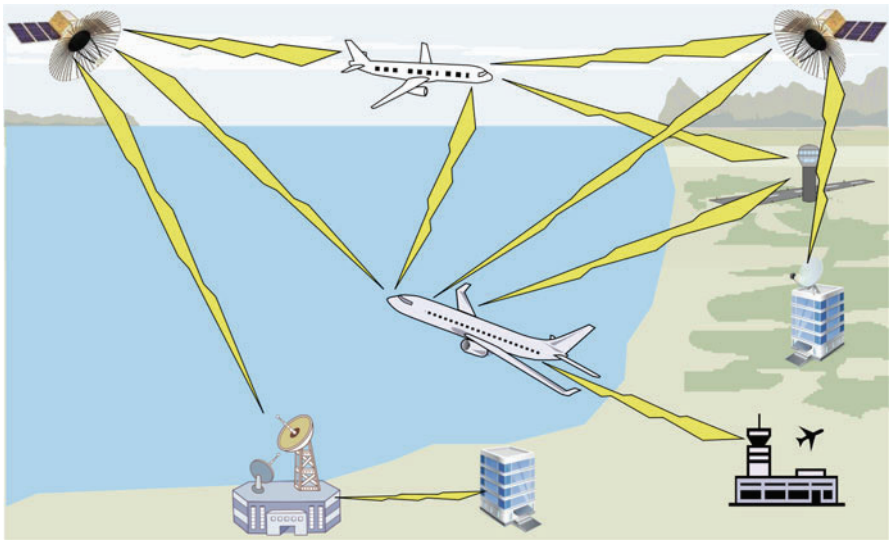

Fig. 7 Crewed aircraft SoS. The aircraft communicates with two satellites to provide (1) in-flight positioning data and telemetry back to a central office, and (2) in-flight live entertainment and Internet access to passengers. The satellites feed data to/from ground stations. Digital and analog links with other aircraft and regional airports allow for two-way communication

Beyond geolocation and other satellite links, communication links also connect aircraft-to-aircraft and aircraft-to-ground stations. For the latter, a modern air traffic management system that uses mutual entity authentication and key agreement based on classical cryptography has been recently introduced [70]. Similarly, it can be expected that future secure aircraft-to-aircraft communication will need to verify digital signatures to check the authenticity of the sending craft or system, to, for example, avoid spamming attacks, where a system's capacity is actively overloaded to force system failure. Given the large number of aircraft that are in transmission range of another aircraft at a given time, large numbers of signatures would need to be signed and verified every second. For instance, an aircraft flying over the Los Angeles Basin or a similar congested airspace at a higher flight level (FL) such as FL330 or above (33,000 feet or above) might receive Automatic Dependent Surveillance—Broadcast (ADS-B) data from hundreds of other aircraft in its communication range (although not all may be displayed on an ADS-B receiver due to the typical ±3500 feet 30 nautical mile "hockey puck" data filtering based on aircraft position [31]) where each aircraft sends a burst of data every 0.5–10 seconds. Hence, it is expected that dedicated chips would be needed to do such cryptographic operations on board the aircraft (an aspect that further hampers post-quantum transition as explained in more detail in Sects. 3.2 and 4.4). A quantum adversary breaking the authenticity or integrity of this communication might be able to change messages to cause mid-air collisions and other high-risk situations. If a quantum adversary could break confidentiality, it would be able to read potentially

sensitive message data either to the aircraft or to entities on-board, creating a potential security risk, for example, in the case of a non-commercial aircraft such as government or defense-related aircraft.

Moving closer to the ground, a quantum adversary could be able to forge digital signatures that should otherwise guarantee the authenticity and integrity of software updates of any of the avionics or control systems. Such software updates are done routinely during maintenance and could cause disturbances during the flight, and in the worst case, cause the aircraft to crash (in back-tracking attacks, an adversary could also tamper with evidence and auditability).

Inside the aircraft, a (very powerful) quantum adversary could be able to also break confidentiality or integrity of the communication on the aircraft itself, for example, between the cockpit and control surfaces such as the wing flaps or between the cockpit and the engine. The data buses inside the aircraft provide a potential avenue of intrusion. For example, an adversary can collect traffic and take it offsite to a quantum computer to extract information (breaking confidentiality and/or integrity) to learn operational information and gain long-term authentication keys. Once keys are derived via quantum cryptanalysis, the adversary would be able to return to the aircraft proximity and potentially take over control of data buses and communication links between the cockpit and, for example, the engines.

5.3 Satellite Systems

As mentioned in the crewed aircraft SoS in Sect. 5.2, satellites provide important communications links. Satellites communicate with aircraft for a variety of purposes such as global satellite navigation (GPS, Global Navigation Satellite System (GLONASS), Galileo, BeiDou, etc.) [71], two-way data for a variety of avionics and crew-ground communications systems (prognostics and health management data for key aircraft systems such as engines, messages to the crew or to the ground pertaining to aircraft operations and notices to aviators, weather reports, etc.), passenger in-flight entertainment system live feeds, passenger Internet access, and others. Back-haul data may constitute such relays for ground stations/aircraft, but also refer to data relayed, for example, across a network of satellites. Satellite system use extends well beyond geolocation and back-haul data applications. Namely, the ability to support such features comes with the need to maintain management of the satellite systems themselves, that is, C2. Naturally, this requires security of the C2 connection for all other features and capabilities to be maintained. With a variety of space systems and communication technologies comes a variety of device lifespans and therefore quantum threat vectors. The system layers and interconnections point to a variety of timeline considerations and post-quantum transition decision point implications.

Some satellites are part of low earth orbit (LEO) constellations that are replaced frequently (every 3–5 years) while other satellites may be in geostationary (GEO) orbits with long lifespans (of 15 or more years). In almost all cases, the hardware

on satellites that is launched into orbit is not field serviceable and remains with the satellite throughout its life. Many satellites have hardware encryption solutions although some may have software encryption solutions that can be updated within the limits of the hardware [6]. In most cases, satellites talk to many different systems—not just aircraft. The satellite transceivers that a satellite uses may be many years old or may be brand new. Also in many cases, satellites must still be able to communicate with legacy transceivers using outdated cryptography. There may be many transceivers that are located in remote areas or are inaccessible so that upgrades cannot be done. When a system is forced to support old cryptographic techniques, downgrade attacks become more likely. All such considerations—difficulty to transition systems and backward compatibility risks—must be accounted for in the system transition plan and post-quantum strategy transition timeline. Hybrid algorithms (described in Sect. 4.5 might offer a way to support older cryptography but also enable security guarantees of post-quantum solutions.

Some satellites may route communications across a back-haul between the transceiver aboard an aircraft and a ground station, as illustrated in Fig. 8. Satellites may have a data link to one or several large ground stations where data is then forwarded to recipients via the Internet, private networks, or other means. Sometimes ground stations are also located in remote regions and are teleoperated, adding yet a further factor into the system diagram of post-quantum transition links. Figure 8 shows a simplified configuration of satellites, ground stations, aircraft, etc.

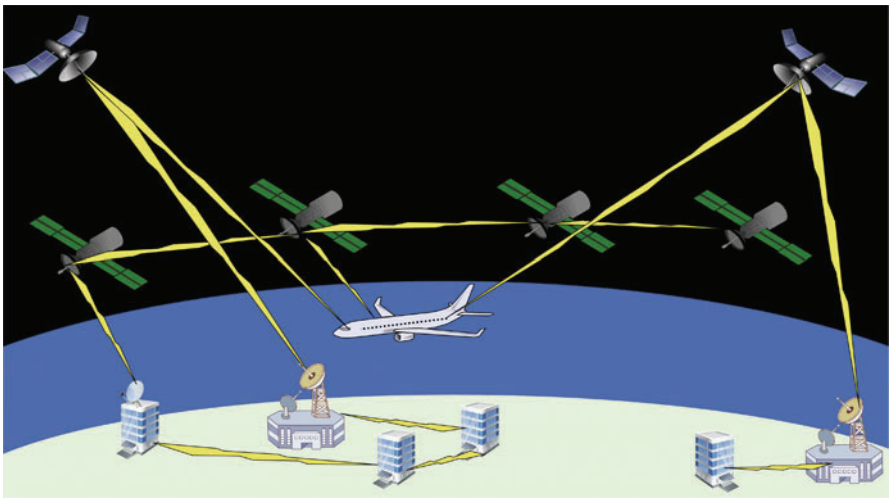

Fig. 8 Satellite CONOPS. A LEO satellite constellation maintains continuous communications with the aircraft and passes data via a back-haul between the satellites to a data link with a ground station that then passes two-way data between the aircraft and a user through the Internet. Two separate GEO satellites communicate with the aircraft and directly to ground stations that relay the communications via the Internet and private networks to users

5.4 Nuclear Power Plants

Most modern nuclear power plants use analog controls for safety-critical systems but digital instrumentation and control (I&C) is coming to some existing plants as well as to-be-constructed plants [42]. Nuclear power plants generate energy from a nuclear fission process—normally via producing steam to spin turbines that generate electricity. In most western nuclear power plant designs, water is used to keep the nuclear fuel rods below 1200°C, which is the point where the zirconium cladding used on most fuel rods begins to decay and can generate hydrogen that produces an explosion risk, and also can lead to the release of radioactive particles into the primary coolant loop [67, 105]. Many sensors are placed throughout a nuclear power plant to monitor all plant systems and help operators to regulate the nuclear reaction taking place in the core. Naturally, safety is essential for a nuclear power plant and any security risks to that are necessarily extremely serious. The safety-critical I&C systems in a nuclear power plant are generally triple redundant to mitigate safety risk. As plants transition legacy systems to digital C2, or even just to digital sensors, the security of such communication links becomes a primary critical protection point.

While the core consideration for many systems is on security transition to post-quantum and matching current system risk profiles to security properties, extreme legacy systems such as nuclear power plants are new to the digital communication space and often currently lack any security protections. As such, there are both benefits and risks to designing for transition now. Potential benefits include the flexibility to design for post-quantum requirements (e.g., key sizes or computational resources) that may eventually be required, especially if any C2 will eventually occur over the air in years to come. Unlike, for example, Internet connections that must be adapted for post-quantum support and integration, such legacy systems are prime for customization at the initiation of security design. On the risk side, however, comes failure to observe the lessons learned in past infrastructure modernization. The Internet of Things is one such example, where previously unconnected devices were "upgraded" to modern connectivity; such connectivity both enabled better command and control of the devices but also introduced security risks—some of which were not well anticipated and planned for [34, 43, 60, 108]. Another issue with nuclear power plants and similar critical and heavily regulated infrastructure is the lengthy review process that must be conducted before changes can be made to core safety systems. Implementing digital I&C within a nuclear power plant may take 10–20 years, and any future changes to I&C systems such as to upgrade to post-quantum cryptographic solutions may take as much or more time. Thus, for legacy systems such as nuclear power plants that are being upgraded now, the core question is, "What current and future threats are being planned for?" When it comes to a quantum threat, the planning and transition timeline is essential.

Concluding this section on case studies regarding the quantum threat and the post-quantum transition, it is important to emphasize that there is a high risk in timelines for the post-quantum transition. This is, in particular, due to only

partial analyses of SoSs by concentrating on some but not all components. Fuller system analysis, such as is done for other risks [40, 73, 74], must proactively undertake inclusion of the quantum threat, with follow-on and urgent actions taken for vulnerable systems. However, this also presents an opportunity; quantum adversaries can be accounted for now in the fundamental threat model base-lining for systems being designed or fundamentally redesigned over the next decades.

6 Conclusion

Quantum computers are an impending threat on the horizon. While the exact timeline of a cryptographically relevant quantum computer is unknown, the consequences for classic asymmetric cryptography would be severe. As system managers and strategic decision-makers consider whether or not to transition to post-quantum secure alternatives, and potential timelines for transition, there are a multitude of factors to consider. Among these are legal and economic implications, system dependencies through data transit of multiple C2 links, the types of security guarantees needed (such as confidentiality and/or integrity), the types of system components needed (hardware processors or software updates), and the integration timeline with respect to data lifespan, post-quantum integration, acquisition, and device lifespan. All of these must be juxtaposed with the wager management takes on for development time of a cryptographically relevant quantum computer—a threat that could become reality in a couple of years, 15 years, 30 years, or any estimate to be placed for risk analysis. What is certain is that a strategic plan is required. Instead of ad hoc decisions limited to the cryptographic layer and subject to the winds of advertisement and marketing jargon, a true system transition plan is based on aggregated security needs and threat risks required for an integrated system in its entirety.

References

1. agnostiq: A Workflow Orchestration Platform Designed for Quantum & HPC (2022). https://agnostiq.ai/covalent/ [Accessed: 2022-03-29]
2. Alagic, G., Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.K., Miller, C., Moody, D., Peralta, R., et al.: Status report on the first round of the NIST post-quantum cryptography standardization process. US Department of Commerce, National Institute of Standards and Technology (2019)
3. Albrecht, M.R., Hanser, C., Höller, A., Pöppelmann, T., Virdia, F., Wallner, A.: Implementing rlwe-based schemes using an RSA co-processor. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2019**(1), 169–208 (2019)
4. An, L., Baynard, C., Chatterjee, C., Loh, C.P.A.: The locational study of atms in the u.s. by ownership (2018). https://www.akleg.gov/basis/get_documents.asp?session=31&docid=22687 [Accessed: 2022-03-29]

5. Anhui Qasky Quantum Technology Co. Ltd.: Qasky (2022). http://www.qasky.com/ [Accessed: 2022-03-29]
6. Banu, P.S.R.: Satellite on-board encryption. Ph.D. thesis, University of Surrey (UK) (2007)
7. Bäuml, S., Christandl, M., Horodecki, K., Winter, A.: Limitations on quantum key repeaters. Nat. Commun. **6**(1), 1–5 (2015)
8. Bernstein, D., Chou, T., Lange, T., von Maurich, I., Misoczki, R., Niederhagen, R., Persichetti, E., Peters, C., Schwabe, P., Sendrier, N., Szefer, J., Wang, W.: Classic mceliece. Tech. rep., Submission to NIST's Post-Quantum Standardization (2019).
9. Bernstein, D.J.: Introduction to post-quantum cryptography. In: Post-Quantum Cryptography, pp. 1–14. Springer, New York (2009)
10. Bernstein, D.J., Buchmann, J., Dahmen, E. (eds.): Post-quantum cryptography. Mathematics and Statistics Springer-11649; ZDB-2-SMA. Springer, New York (2009)
11. Beullens, W.: Breaking rainbow takes a weekend on a laptop. Cryptology ePrint Archive, Report 2022/214 (2022). https://ia.cr/2022/214
12. Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., Stebila, D.: Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange. In: J. Ding, R. Steinwandt (eds.) Post-Quantum Cryptography—10th International Conference, PQCrypto 2019, Chongqing, China, May 8–10, 2019 Revised Selected Papers. Lecture Notes in Computer Science, vol. 11505, pp. 206–226. Springer (2019)
13. Bindel, N., Herath, U., McKague, M., Stebila, D.: Transitioning to a quantum-resistant public key infrastructure. In: T. Lange, T. Takagi (eds.) Post-Quantum Cryptography—8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26–28, 2017, Proceedings. Lecture Notes in Computer Science, vol. 10346, pp. 384–405. Springer (2017)
14. Boneh, D.: Twenty years of attacks on the rsa cryptosystem. Not. AMS **46**, 203–213 (1999)
15. Bos, J.W., Costello, C., Naehrig, M., Stebila, D.: Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In: 2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17–21, 2015, pp. 553–570. IEEE Computer Society (2015)
16. Brendel, J., Fiedler, R., Günther, F., Janson, C., Stebila, D.: Post-quantum asynchronous deniable key exchange and the signal handshake. In: G. Hanaoka, J. Shikata, Y. Watanabe (eds.) Public-Key Cryptography – PKC 2022, pp. 3–34. Springer International Publishing, Cham (2022)
17. Cabinet Office, U.G.: Government Security Classifications May 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment/data/file/715778/May-2018/Government-Security-Classifications-2.pdf (2018). Accessed: 2022-03-27
18. Chen, L., Jordan, S., Liu, Y.K., Moody, D., Peralta, R., Perlner, R., Smith-Tone, D.: Nistir 8105 report on post-quantum cryptography. Tech. rep., National Institute for Standards and Technology (NIST) (2016)
19. Chen, L., Moody, D., Liu, Y.K.: Post-quantum cryptography. Tech. rep., National Institute of Standards (NIST) (2016)
20. Chen, L., Moody, D., Liu, Y.K.: Post-quantum cryptography calls for proposal. Tech. rep., National Institute of Standards (NIST) (2017)
21. Crockett, E., Paquin, C., Stebila, D.: Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH. Cryptology ePrint Archive, Report 2019/858 (2019). https://ia.cr/2019/858
22. Csenkey, K., Bindel, N.: Post-quantum cryptographic assemblages and the governance of the quantum threat (2021). https://doi.org/10.31235/osf.io/3ws6p
23. Gueron, S., Stebila, D., Fluhrer, S.: Hybrid key exchange in tls 1.3, internet draft. Tech. rep., Internet Engineering Task Force (IETF) (2022)
24. Degabriele, J.P., Lehmann, A., Paterson, K.G., Smart, N.P., Strefler, M.: On the joint security of encryption and signature in EMV. In: O. Dunkelman (ed.) Topics in Cryptology—CT-RSA 2012—The Cryptographers' Track at the RSA Conference 2012, San Francisco, CA, USA, February 27–March 2, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7178, pp. 116–135. Springer (2012)

25. Ding, J., Chen, M., Petzoldt, A., Schmidt, D., Yang, B., Kannwischer, M., Patarin, J.: Rainbow. Tech. rep., Submission to NIST's Post-Quantum Standardization (2020)
26. Dowling, B., Hale, B.: There can be no compromise: The necessity of ratcheted authentication in secure messaging. IACR Cryptol. **2020**, 541 (2020). ePrint Arch
27. Esser, A., May, A., Verbel, J., Wen, W.: Partial key exposure attacks on bike, rainbow and ntru. Cryptology ePrint Archive, Report 2022/259 (2022). https://ia.cr/2022/259
28. ESTI: Etsi ts 103 744 v1.1.1, cyber; quantum-safe hybrid key exchanges. Tech. rep., European Telecommunications Standards Institute (ETSI) (2020)
29. eVisit: The Ultimate HIPAA Guide: The Facts You Need to Know (2022). https://evisit.com/resources/hipaa-guide/ [Accessed: 2022-03-29]
30. Faruk, M.J.H., Miner, P., Coughlan, R., Masum, M., Shahriar, H., Clincy, V., Cetinkaya, C.: Smart connected aircraft: Towards security, privacy, and ethical hacking. In: 2021 14th International Conference on Security of Information and Networks (SIN), vol. 1, pp. 1–5. IEEE (2021)
31. Federal Aviation Administration: Nextgen equip ads-b ins and outs (2021). https://www.faa.gov/nextgen/equipadsb/capabilities/ins_outs/ [Accessed: 2022-03-29]
32. Federal Office for Information Security: Migration zu post-quanten-kryptografie handlungsempfehlungen des bsi (german). Tech. rep., Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020)
33. Feo, L.D., Jao, D., Plût, J.: Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. J. Math. Cryptol. **8**(3), 209–247 (2014)
34. Frustaci, M., Pace, P., Aloi, G., Fortino, G.: Evaluating critical security issues of the iot world: Present and future challenges. IEEE Internet Things J. **5**(4), 2483–2495 (2017)
35. Fuchs, C.M., et al.: The evolution of avionics networks from ARINC 429 to AFDX. In: Innovative Internet Technologies and Mobile Communications (IITM), and Aerospace Networks (AN), vol. 65, pp. 1551–3203 (2012)
36. Gibney, E.: The quantum gold rush. Nature **574**(7776), 22–24 (2019)
37. Gidney, C., Ekerå, M.: How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. Quantum **5**, (2021). https://doi.org/10.22331/q-2021-04-15-433
38. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: G.L. Miller (ed.) Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22–24, 1996, pp. 212–219. ACM (1996)
39. Haggard, S., Lindsay, J.R.: North korea and the sony hack: Exporting instability through cyberspace. Analysis from the East-West Center (2015). https://www.jstor.org/stable/resrep06456
40. Hale, B., Van Bossuyt, D.L., Papakonstantinou, N., O'Halloran, B.: A zero-trust methodology for security of complex systems with machine learning components. In: International Design Engineering Technical Conferences and Computers and Information in Engineering Conference, vol. 85376, p. V002T02A067. American Society of Mechanical Engineers (2021)
41. Harkins, D.: Dragonfly key exchange. Tech. rep., Internet Research Task Force (IRTF) (2015)
42. Hashemian, A., Arnholt, B.: Nuscale power module instrumentation. Nucl. Plant J. (Online) **36**(4), (2018)
43. Hassan, W.H., et al.: Current research on internet of things (iot) security: A survey. Comput. Netw. **148**, 283–294 (2019)
44. Huelsing, A., Butin, D., Gazdag, S., Rijneveld, J., A., M.: Mss: Extended hash-based signatures. Tech. rep., RFC 8391 (2018)
45. Huhnlein, D., Korte, U., Langer, L., Wiesmaier, A.: A comprehensive reference architecture for trustworthy long-term archiving of sensitive data. In: 2009 3rd International Conference on New Technologies, Mobility and Security, pp. 1–5. IEEE (2009)
46. Humboldt University Berlin SarWiki: WPA3 Dragonfly Handshake (2022). https://sarwiki.informatik.hu-berlin.de/WPA3_Dragonfly_Handshake [Accessed: 2022-03-29]
47. IDQ: Cerberis XG QKD system: quantum key distribution for enterprise, government and telco production environments (2022). https://www.idquantique.com/quantum-safe-security/products/cerberis-xg-qkd-system/ [Accessed: 2022-03-29]

48. IEEE: Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments (2010). IEEE Standard 802.11p
49. InfiniQuant: InfiniQuant (2022). https://infiniquant.com/ [Accessed: 2022-03-29]
50. Information Security Oversight Office, N.A., Administration, R.: ISOO Notice 2017-02: Clarification of Classification by Compilation. https://www.archives.gov/files/isoo/notices/notice-2017-02.pdf (2017). Accessed: 2022-03-27
51. Joux, A., Odlyzko, A., Pierrot, C.: The past, evolving present, and future of the discrete logarithm. In: Open Problems in Mathematics and Computational Science, pp. 5–36. Springer (2014)
52. Kadet, K.: Entrust. Entrust Helps Enterprises Prepare Now for Post Quantum Security Journey with New PQ Testing and Development Solutions (2022). https://www.entrust.com/newsroom/press-releases/2022/entrust-helps-enterprises-prepare-now-for-post-quantum-security-journey [Accessed: 2022-03-29]
53. Katz, J., Lindell, Y.: Introduction to Modern Cryptography. Chapman and Hall/CRC Press, London (2007)
54. Kelly, J.: A Preview of Bristlecone, Google's New Quantum Processor. https://ai.googleblog.com/2018/03/a-preview-of-bristlecone-googles-new.html (2018). Accessed: 2018-07-23
55. KETS Quantum: KETS (2022). https://kets-quantum.com/ [Accessed: 2022-03-29]
56. Krishna, C.L., Murphy, R.R.: A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In: 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), pp. 194–199. IEEE (2017)
57. Lynch, C.: Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust. Routledge, New York (2013)
58. MacQuarrie, E.R., Simon, C., Simmons, S., Maine, E.: The emerging commercial landscape of quantum computing. Nat. Rev. Phys. **2**(11), 596–598 (2020)
59. MagiQ Tech: MagiQ (2022). https://www.magiqtech.com/ [Accessed: 2022-03-29]
60. Mahmoud, R., Yousuf, T., Aloul, F., Zualkernan, I.: Internet of things (iot) security: Current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 336–341. IEEE (2015)
61. Mavroeidis, V., Vishi, K., Zych, M.D., Jøsang, A.: The impact of quantum computing on present cryptography. Preprint (2018). arXiv:1804.00200
62. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, London (2018)
63. Michele Mosca, J.M.: A methodology for quantum risk assessment (2017). https://globalriskinstitute.org/publications/3423-2/ [Accessed: 2022-03-29]
64. Moir, I., Seabridge, A.: Design and Development of Aircraft Systems, vol. 67. Wiley, New York (2012)
65. Mosca, M.: Cybersecurity in an era with quantum computers: Will we be ready? IEEE Secur. Priv. **16**(5), 38–41 (2018)
66. Moteff, J., Parfomak, P.: Critical infrastructure and key assets: definition and identification. Tech. rep., Library of Congress Washington DC Congressional Research Service (2004)
67. Motta, A.T., Capolungo, L., Chen, L.Q., Cinbiz, M.N., Daymond, M.R., Koss, D.A., Lacroix, E., Pastore, G., Simon, P.C.A., Tonks, M.R., et al.: Hydrogen in zirconium alloys: A review. J. Nucl. Mater. **518**, 440–460 (2019)
68. Mumtaz, M., Ping, L.: Forty years of attacks on the rsa cryptosystem: A brief survey. J. Discrete Math. Sci. Cryptogr. **22**(1), 9–29 (2019)
69. Murdoch, S.J., Drimer, S., Anderson, R.J., Bond, M.: Chip and PIN is broken. In: 31st IEEE Symposium on Security and Privacy, S&P 2010, 16–19 May 2010, Berleley/Oakland, California, USA, pp. 433–446. IEEE Computer Society (2010)
70. Mäurer, N., Gräupl, T., Schmitt, C.: L-band Digital Aeronautical Communications System (LDACS). Internet-Draft draft-ietf-raw-ldacs-10, Internet Engineering Task Force (2022). Work in Progress

71. National Coordination Office for Space-Based Positioning, Navigation, and Timing: GPS.GOV: Official U.S. government information about the Global Positioning System (GPS) and related topics: Space Segment (2022). https://www.gps.gov/systems/gps/space/ [Accessed: 2022-03-29]
72. Neuman, B.C., Ts'o, T.: Kerberos: An authentication service for computer networks. IEEE Commun. Mag. **32**(9), 33–38 (1994)
73. Papakonstantinou, N., Hale, B., Linnosmaa, J., Salonen, J., Van Bossuyt, D.L.: Model driven engineering for resilience of systems with black box and ai-based components. In: Reliability and Maintainability Symposium (2022)
74. Papakonstantinou, N., Van Bossuyt, D.L., Linnosmaa, J., Hale, B., O'Halloran, B.: A zero trust hybrid security and safety risk analysis method. J. Comput. Inf. Sci. Eng. **21**(5), 1–26 (2021)
75. Paquin, C., Stebila, D., Tamvada, G.: Benchmarking post-quantum cryptography in TLS. In: J. Ding, J. Tillich (eds.) Post-Quantum Cryptography—11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings. Lecture Notes in Computer Science, vol. 12100, pp. 72–91. Springer (2020)
76. Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al.: Advances in quantum cryptography. Adv. Opt. Photon. **12**(4), 1012–1236 (2020)
77. Pittaluga, M., Minder, M., Lucamarini, M., Sanzaro, M., Woodward, R.I., Li, M.J., Yuan, Z., Shields, A.J.: 600-km repeater-like quantum communications with dual-band stabilization. Nat. Photon. **15**(7), 530–535 (2021)
78. Post Quantum: Simple, secure, now (2022). https://www.post-quantum.com/ [Accessed: 2022-03-29]
79. PQShield: Understanding the quantum threat, post-quantum cryptography and the upcoming NIST standards (2022). https://pqshield.com/quantum-threat/ [Accessed: 2022-03-29]
80. Qabacus: Welcome to the Future Website of Qabacus Blockchain! (2022). https://www.qabacus.com/ [Accessed: 2022-03-29]
81. Qaisec: Quantum encryption and AI (2022). http://www.qaisec.eu/ [Accessed: 2022-03-29]
82. QBT: Quantum Blockchain Technologies (2022). https://quantumblockchaintechnologies.co.uk/ [Accessed: 2022-03-29]
83. QRATE: Quantum Solutions (2022). https://qrate.online/ [Accessed: 2022-03-29]
84. Qrypt: Eternal Encryption (2022). https://www.qrypt.com/ [Accessed: 2022-03-29]
85. Quantique, C.: Scalable IoT security from chip to cloud (2022). https://www.cryptoquantique.com/ [Accessed: 2022-03-29]
86. Quantum Dice: Securing a Connected Future (2022). https://quantum-dice.com/ [Accessed: 2022-03-29]
87. Quantum Xchange: Delivering the Future of Encryption (2022). https://quantumxc.com/ [Accessed: 2022-03-29]
88. QuBalt: Security Solutions for the Quantum Internet, Quantum Key Distribution Networks and Safety-Critical Systems (2022). https://www.qubalt.de/ [Accessed: 2022-03-29]
89. QuSecure: Scalable Cybersecurity for the Post-Quantum Enterprise (2022). https://www.qusecure.com/ [Accessed: 2022-03-29]
90. Räsänen, M., Mäkynen, H., Möttönen, M., Goetz, J.: Path to european quantum unicorns. EPJ Quantum Technol. **8**(1), 5 (2021)
91. Rivest, R.L., Shamir, A., Adleman, L.M.: A method for obtaining digital signatures and public-key cryptosystems (reprint). Commun. ACM **26**(1), 96–99 (1983)
92. Robling Denning, D.E.: Cryptography and Data Security. Addison-Wesley Longman Publishing Co., Boston (1982)
93. Sampigethaya, K., Poovendran, R., Shetty, S., Davis, T., Royalty, C.: Future e-enabled aircraft communications and security: The next 20 years and beyond. Proc. IEEE **99**(11), 2040–2055 (2011)
94. Shaikh, F., Rahouti, M., Ghani, N., Xiong, K., Bou-Harb, E., Haque, J.: A review of recent advances and security challenges in emerging e-enabled aircraft systems. IEEE Access **7**, 63164–63180 (2019)

95. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Rev. **41**(2), 303–332 (1999)
96. Sikeridis, D., Kampanakis, P., Devetsikiotis, M.: Post-quantum authentication in TLS 1.3: A performance study. In: 27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23–26, 2020. The Internet Society (2020)
97. Simmons, G.J.: Symmetric and asymmetric encryption. ACM Comput. Surv. (CSUR) **11**(4), 305–330 (1979)
98. Srivastava, R., Choi, I., Cook, T., Team, N.U.E.: The Commercial Prospects for Quantum Computing. Networked Quantum Information Technologies (2016)
99. Support, D.: Apps and Keys (2022). https://support.docusign.com/guides/ndse-admin-guide-api-and-keys [Accessed: 2022-03-29]
100. Van Meter, R.: Security of quantum repeater network operation. Tech. rep., Keio University Fujsawa Japan (2016)
101. Van Tilborg, H.C., Jajodia, S.: Encyclopedia of Cryptography and Security. Springer Science & Business Media, New York (2014)
102. Vanhoef, M., Ronen, E.: DRAGONBLOOD: Analysing WPA3's Dragonfly Handshake (2022). https://wpa3.mathyvanhoef.com/ [Accessed: 2022-03-29]
103. VeriQloud: Quantum Cybersecurity Unlocked (2022). https://veriqloud.com/ [Accessed: 2022-03-29]
104. Windows App Development: Microsoft Kerberos (2022). https://docs.microsoft.com/en-us/windows/win32/secauthn/microsoft-kerberos Accessed: 2022-03-29]
105. Yanez, J., Kuznetsov, M., Souto-Iglesias, A.: An analysis of the hydrogen explosion in the fukushima-daiichi accident. Int. J. Hydrogen Energy **40**(25), 8261–8280 (2015)
106. Yun, A., Shi, C., Kim, Y.: On protecting integrity and confidentiality of cryptographic file system for outsourced storage. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, pp. 67–76 (2009)
107. Zetter, K.: Feds Say That Banned Researcher Commandeered a Plane (2015)
108. Zhang, Z.K., Cho, M.C.Y., Wang, C.W., Hsu, C.W., Chen, C.K., Shieh, S.: Iot security: ongoing challenges and research opportunities. In: 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230–234. IEEE (2014)